



# Simulation-supported aviation cyber-security risk analysis: a case study

A. R. Schmitt<sup>1</sup> · C. Edinger<sup>1</sup> · T. Mayer<sup>2</sup> · J. Niederl<sup>3</sup> · T. Kiesling<sup>4</sup>

Received: 11 December 2017 / Revised: 17 August 2018 / Accepted: 25 September 2018 / Published online: 6 October 2018  
© Deutsches Zentrum für Luft- und Raumfahrt e.V. 2018

## Abstract

The air transport infrastructure is important and prominent. The current aviation system is already vulnerable and the advent of more automation and pervasion of standard IT in the future leads to ever more complex and interconnected systems with an increasing attack surface. To cope with this situation, we need suitable methods and tools to achieve understanding of the consequences in potential cyber threat situations. In this paper, we present results of a case study on the use of simulation methodologies to support aviation cyber-security risk assessment. We use different variants of a flight plan data manipulation scenario as well as a scenario, where the availability of flight plan data is compromised. The one day scenarios were implemented in the air traffic simulator TrafficSim. The aim is to investigate the potential of the methodology and to achieve an estimation of cyber-threat potentials in connection with flight plan data processing. One scenario capped the flight level of 473 flights on the same airway, resulting in 1073 t additional fuel, and 147 flights would spend their minimum final reserve fuel before landing. A second scenario showed that four or five flights, missing their flight plan at startup, could impact a well utilized runway for about 2–4 h. During a risk assessment, the effects of an attack can be more accurately assessed using simulation results. We recommend to (1) develop, maintain, and apply simulation models and cyber attack simulation scenarios, (2) connect and develop simulation models from “gate-to-gate”, and (3) integrate human interactions with cyber attack simulation scenarios.

**Keywords** ATM security · Air traffic simulation · Risk analysis · Missing or manipulated flight plan

## 1 Introduction

Cyber security in all its facets is not a new issue. It has been considered in various aspects for quite a long time, typically with a focus on technological aspects. Nowadays, it is largely recognized, that among other effects, cyber threats could be targeting critical infrastructures such as energy supply, telecommunications, or transport. The aviation system as part of the transport critical infrastructure is an attractive target, both in terms of its publicity as well as its importance. This is reflected in increased efforts to define and implement

necessary security measures, especially in the context of air navigation service provision [1].

### 1.1 Background and scope

We will use the term ‘aviation cyber security’ to encompass all viable protective measures against potential cyber threats targeting the global air transport system or parts of it. We will further differentiate between preventive measures (intended to prevent threat actors to successfully infiltrate systems) and resilience measures (limiting the effectiveness of successful intrusions). It is a matter of ongoing debate whether the current air transport system is effectively protected against cyber attacks that can result in aircraft crashes or similar catastrophic events. However, there are other types of cyber threats in air transport that have materialized like delays due to faulty ground systems (e.g., in the US [2]) or due to goal-oriented attacks (e.g., in Warsaw [3]).

The advent of modern technology is manifested among others in the development of the next generation of Air

✉ A. R. Schmitt  
Angela.Schmitt@dlr.de

<sup>1</sup> German Aerospace Center e.V., Brunswick, Germany

<sup>2</sup> Universität der Bundeswehr München, Munich, Germany

<sup>3</sup> IABG, Ottobrunn, Germany

<sup>4</sup> Airbus, Ottobrunn, Germany

Traffic Management (ATM) systems (in Europe especially towards a Single European Sky through the SESAR program) as well as ever more thoroughly interconnected and automated systems. These trends have positive effects in terms of the improvement of stakeholder experience as well as the increase in efficiency and capacity of the overall air traffic system. On the downside, the growing system complexity leads to an ever-increasing attack surface, as well. To cope with this situation, we need effective risk-based approaches to security. Unfortunately, classical risk assessment methodologies employed in the context of information security (see for instance [4]) are not well suited for the analysis of complex system-of-systems. The first and foremost challenge here is the understanding of aviation as a socio-technical system, that is a functional system integrating people, rules and technical systems. A holistic approach has to consider all essential sub-systems and their interdependencies in the context of potential threat situations. What we need as basic building blocks are proper methods and tools for a holistic threat and risk assessment.

This motivated the Air Traffic Resilience (ARIEL) project team to evaluate scenario-oriented and model-based methods for aviation cyber-security risk assessment [5]. To accommodate the diversity of potential threats and the complexity of the aviation system, the project uses an approach based on an exemplary choice of cyber-threat scenarios and an aggregated representation of the aviation system. In its first phase, the focus of activities in ARIEL was on the procedures and methods for dynamic security risk assessment [6] as well as internal and external aircraft communication.

For several years now, the security community intensified efforts to research vulnerabilities, threats, and potential attacks on the aviation system at large and air traffic control specifically [7]. There have been numerous findings about potentially insecure standards and systems. However, with the absence of large-scale incidents clearly originating from cyber attacks, the aviation community has frequently doubted the possibility of these kinds of attacks either being realistic in the first place or leading to serious impacts in the second place [8–10]. Currently, there exists a gap in understanding of potential threat scenarios between the security community and the aviation community, or as Strohmeier et al. state: “...many who understand [...] security, do not have appropriate aviation expertise. Likewise, many stakeholders in aviation know the processes and procedures but do not realize the severity of modern cyber-security issues” [7, p. 1339].

The excellent work of Strohmeier et al., for instance, tries to tackle this challenge by collecting a comprehensive body of knowledge about wireless security in aviation and conducting wide-spread interviews with experts in the aviation community. This is definitely the right direction, but

from our experience in conducting security research in the aviation world, effective communication with aviation stakeholders needs to be based on concrete examples of cyber attacks including illustrations of their effects on the aviation processes and procedures.

We do believe that simulation methodologies are an excellent means to analyse impacts of cyber-threat scenarios, but even more importantly to illustratively convey their implications to aviation stakeholders. Therefore, the second phase of the ARIEL project was dedicated to the exploration of simulation methodologies to support cyber-security risk analysis in aviation. The major results of one case study are presented in this paper.

## 1.2 Threat scenarios and model

This contribution presents the analysis of threat potentials. For that analysis, we prioritized two different attack scenarios from phase one which focus on the integrity and availability of flight plan data. Both scenarios attack the flight plan exchange system. The first scenario assumes the possibility of intentional manipulations of the planned cruise flight level used for air traffic control. The second scenario includes the intentional deletion of flight plans of certain flights shortly before their departure at the origin airport. The air traffic simulator TrafficSim from the German Aerospace Center (DLR) is used to simulate the airborne processes including the effects of the assumed cyber attack actions. Both scenarios were implemented in that simulator. Measurable deviations in a threat scenario are, for example, duration of flight, airspace sectors used and fuel consumption. Especially, the level capping can lead to a complete consumption of the trip fuel and may cause an emergency.

The scenarios are inspired by abnormal system behavior caused by unintentional acts like weather, technical issues, or human errors. We anticipate that abnormal system behavior can also be caused by cyber attacks. We assume an attacker is able to infiltrate the communication channel between IFPS and ATC units to modify flight plan data. Based on this assumption, we focus on the potential consequences in such a case. Note that we did not perform any kind of technical vulnerability assessment on real ATM/ATC communication systems. Therefore, we do not give any indication on the likelihood of such an event, we just evaluate potential impacts and obtain conclusions for the risk assessment in the context of our scenarios.

Of course, it is arguable whether such a kind of attack is likely in the current air traffic management system. To realize an attack vector achieving the results that we assume on the ATM/ATC communication, rather well protected ATM/ATC systems need to be infiltrated. This can only be done by knowledgeable and/or well-resourced threat actors. For our

scenarios, we assume the presence of an insider threat, the likelihood of which has been well discussed in IT contexts [11] as well as in the aviation sector [12]. We generally deem an insider threat as likely enough to achieve the necessary plausibility of our threat scenarios.

Note that the scope of our study is the demonstration of the utility of simulation methods to aid threat impact analysis for the support of cyber-security risk analysis. To this end, the threat scenarios are well suited due to their general plausibility as well as their closeness to abnormal system behavior that is frequently experienced by ATC staff and/or aircraft crews.

This paper continues with a short discussion of related work. The setup for the simulation experiments is described in Sect. 3. The use case scenarios are introduced in Sect. 4. Section 5 presents the experiment results. We summarized our experiences with this simulation in recommendations for future activities in Sect. 6. This paper ends with concluding discussions in Sect. 7.

## 2 Related work

To analyse potential impacts on operational air transport processes, cyber-threat scenarios were developed within the project ARIEL [5]. These processes contain all aircraft life-cycle processes from manufacturing to deployment to maintenance based on European ATM Architecture. Our research focuses on ATM controlled and observed processes only. We group these processes into three main categories: planning, ground, and airborne processes. We consider a pre-planning and a post-planning phase as parts of the planning processes and a pre-ground and post-ground phase as parts of the ground processes. Note that these processes influence and interact with each other. For example, a delayed “Take-off & Departure” (airborne process) will probably cause a delayed “Taxi-in” (ground process).

Simulation is an established methodology to investigate and evaluate complex systems and create a reliable communication basis for experts from different domains [13, 14]. This is also true in the domain of ATM [15]. For example, short-term operational planning as part of the planning process is addressed with simulation in [16]. A simulation-based method to solve the Aircraft Turnaround Problem is introduced in [17]. Human-in-the-loop (HITL) simulations are performed to evaluate, e.g., new ATM concepts like Next Generation Air Transportation System (NextGen) in the Airspace Operations Laboratory at NASA Ames Research Center [18] or the SESAR program at EUROCONTROL [19]. HITL simulations focus on human interactions during the simulation, in not HITL simulations those interactions are often modelled with assumptions or simplifications. Especially, in the area of air traffic management and flight

execution, these interactions are frequently the object of study in a simulation experiment.

In general, the observed processes show different characteristics and are, therefore, addressed with different kinds of simulation. Several taxonomies of computer simulation exist. Most taxonomies distinguish Discrete Event Simulation (DES) from Continuous Simulation [20]. Special forms are system dynamics and agent-based modelling. Hybrid systems are usually challenging and require a combination of these types [21–23]. The analysis of ground or planning processes is a typical field of application for DES with stochastic inputs. Main characteristic of DES is that the system state only changes due to events triggered at a certain point in time. Continuous simulation characterises a continuously changing system state. An application area of continuous simulation is the analysis of airborne processes, in the context of ATM. “System dynamics is a high level simulation paradigm that utilizes a continuous simulation implementation scheme together with mathematical modelling techniques” [24] introduced from Professor Jay Forrester in the mid-1950s [25]. Agent-based modelling is also a high level simulation paradigm. An agent is an active, autonomous, or semi-autonomous model component, which has the ability to communicate with other agents and with the environment [26].

Since the early work from [27] in 1999, simulation is also applied in the context of cyber security. For example, [28] developed a network security simulation that is able to classify threats, specify attack mechanisms, verify protection mechanisms, and evaluate consequences. Attacker behavior was integrated into IT security analyses with the help of a DES approach by [29]. In the context of ATM processes, cyber-security simulation is established as well. For example, the Global ATM Security Management project (GAMMA) [30] deals with a holistic approach for ATM security management. A comprehensive security risk analysis identifies present and near future risks of ATM systems. Based on that, different prototypes for security or threat detection were implemented and validated. However, at the 27th meeting of the Aviation Security Panel in Montreal, the International Civil Aviation Organization emphasized also the importance of understanding systems behavior when a cyber attack actually happens. This demand is addressed by [31], by developing a simulation/emulation framework to evaluate the effects of cyber attacks and network/communication failures on Air Traffic Control (ATC). Their work focuses on an attack at a technical level. The simulated cyber attack injects false targets into the automatic dependent surveillance—broadcast receivers, to deceive air traffic controllers and threaten ATM.

Our research is not focusing on the technical details of cyber attacks themselves. Rather, it concentrates on the

effects of a potential cyber attack on system level. Since our simulations model airborne processes with no interaction to other process types, we chose the continuous simulator TrafficSim for the execution of our simulations. Note that HITL simulations were not part of our research.

### 3 Air traffic simulation

An air traffic simulation can be composed of many models focusing on specified applications (arrival and departure manager, ground movements, ATC, etc.). The simulations introduced in this paper focus on airborne processes only. Ground processes like ground movements, passenger behavior, or aircraft turnaround (e.g., delay of an aircraft postpones the next flight of that aircraft) are not considered. This section differentiates and describes the applied simulation model.

The air traffic simulation software called TrafficSim from DLR was used for our experiments. TrafficSim is designed to support the development and validation of on-board as well as ATM tools. It is suitable as a “proof of concept simulation” for new ATM concepts and trajectory-based operations. TrafficSim is able to simulate airborne processes and is capable to handle realistic aircraft movements as well as to process high traffic scenarios with more than 70,000 aircraft in real- or fast time. Each simulated aircraft is equipped with DLR’s 4D-Flight Management System (FMS) that guides the aircraft along its generated 4D-trajectory automatically and accurately in time. In the scenarios, flights are conflict-free considering defined separation minima. Pre-tactical and tactical tools are utilized by TrafficSim to comply with flight plans and consider runway occupancy times, as described in this section.

#### 3.1 4D-FMS in TrafficSim

The prediction of the flight trajectory comprises

1. the generation of the route description (2D trajectory) for a given set of waypoints contained in the flight plan;
2. the generation of altitude (3D trajectory) and airspeed profile according to the given performance parameters;
3. the calculation of ground speed, range, and flight time (4D trajectory).

The lateral route is made up of geodesic legs between waypoints and arcs with a fixed radius at the waypoints. All calculations are based on the World Geodetic System 84. Vincenty’s formulae are used to calculate distance and track between route points of the 2D trajectory. The vertical profile consists of a sequence of flight phases: climb,

level flight (cruise), descent, combined with constant speed, acceleration, or deceleration phases. The climb is predicted at high power setting. The descent is planned with idle power setting. Altitude and airspeed profile are predicted by integration of the equations of motion for each sub phase. The operation performance data used by the aerodynamic and engine thrust models are read from Base of Aircraft Data (BADA) Revision 3.12 provided by EUROCONTROL [32]. The vertical profile is predicted using a nominal speed profile specified in BADA for the individual aircraft type. No airline procedures (e.g., climb profiles) are considered. A low drag/low-power approach profile is used for all predicted 4D trajectories.

The 4D-FMS was validated in flight trials with DLR’s research aircraft ATTAS (VFW614), ATRA (A320), and in the A330 full flight simulator of Zentraler Flugsimulator Berlin [33–35].

#### 3.2 Separation and conflict detection

Flight trajectories are laterally and vertically separated by defined separation minima. A conflict exists if a separation falls below the minimum. In general, the separation in the en-route airspace is 5 nautical miles radius laterally and 1000 ft vertically. Exceptions are oceanic, approach, or non-radar environments. For conflict detection, an additional safety margin of one nautical mile (NM) is added to the requested lateral separation. Therefore, a separation cylinder of 6 NM radius laterally and 1000 ft vertically is assigned to each aircraft and is not allowed to intersect with any other separation cylinder. The built-in 4D conflict detection tool efficiently checks for conflicts in en-route airspace. Core of this tool is a patent-protected method for determining a potential conflict situation between objects within a multi-dimensional traffic area [36, 37].

One aircraft may be involved in different conflicts along its route. If an aircraft is involved in several different conflicts with other aircraft in an observation interval of 15 min, we will call this a multiple conflict.

#### 3.3 Airport slot manager

The built-in Airport Slot Manager is a pre-tactical planning tool, and assigns each aircraft a landing or take-off slot considering wake categories and runway occupancy time. For each aircraft on ground, the take-off time is shifted to meet the assigned landing/take-off slot, trying to closely meet the take-off time in the flight plan. For aircraft already airborne, a top-of-descent time constraint is calculated and set, so that deviations are corrected before reaching the extended Terminal Maneuvering Area (TMA) and the landing slot will be met with standard approach speeds. After entering the

**Table 1** Defined separation minima depending on wake turbulence between aircraft

Minimum separation in NM	Following aircraft		
	Heavy	Medium	Light
Preceding aircraft			
Heavy	4	5	6
Medium	3	3	5
Light	3	3	3

extended TMA, the aircraft is handed over to the Arrival/Departure Manager to check and correct the separation between two aircraft in the approach and departure phases of flight. It is assumed that the separation minima between arriving and following departing aircraft called *runway occupancy time* are 75 s. All other separation minima are set to the wake turbulence separation minima described in Table 1.

If a faster aircraft departs after a slower aircraft, an additional offset is added to the take-off time to avoid the distance between both departures being shortened immediately after take-off. If there is a block of departures with more than two aircraft and one aircraft is much slower than the others, the slow aircraft is shifted to the end of the departure block.

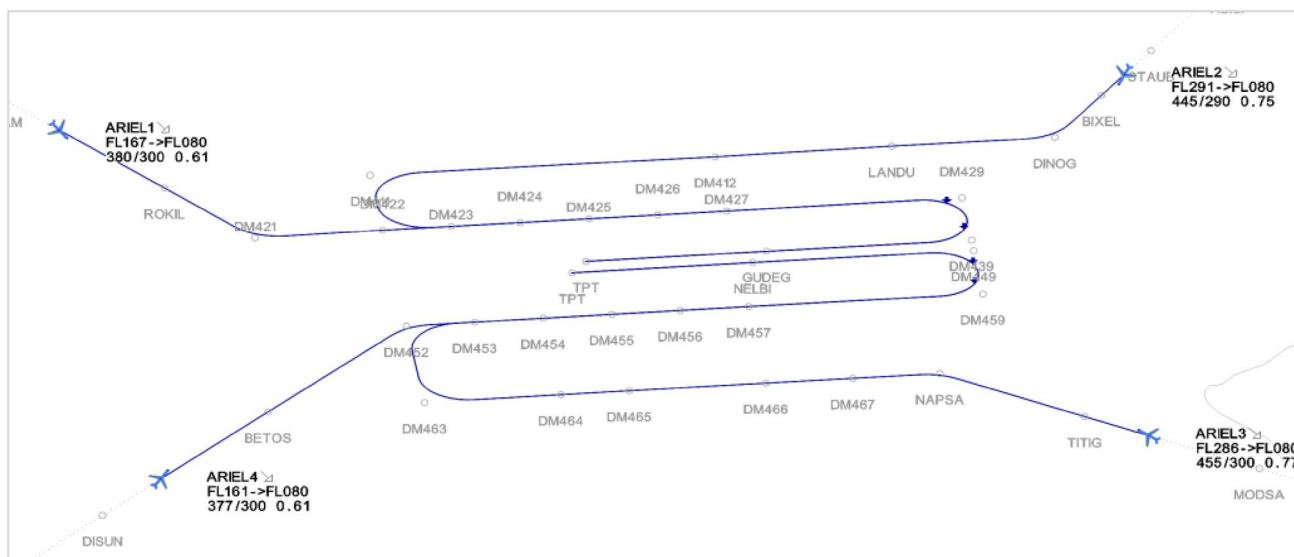
### 3.4 Arrival and departure manager (AMAN and DMAN)

The built-in AMAN/DMAN is a tactical planning tool, which updates assigned landing or take-off times to react on short-term events or deviations from the pre-planned 4D-trajectories. Departures are rescheduled after a slot-effecting event according to the take-off time specified in the filed flight plan (e.g., take-off delay). The touchdown times of arrivals are updated after a slot-effecting event occurred but at least when the aircraft enters the extended TMA (150 NM). TrafficSim recalculates the affected trajectories using path stretching or holding circuits to meet assigned touchdown times. All touchdown and take-off times are calculated considering the slot constraints described in the preceding section.

### 3.5 Departure and arrival routes at Munich

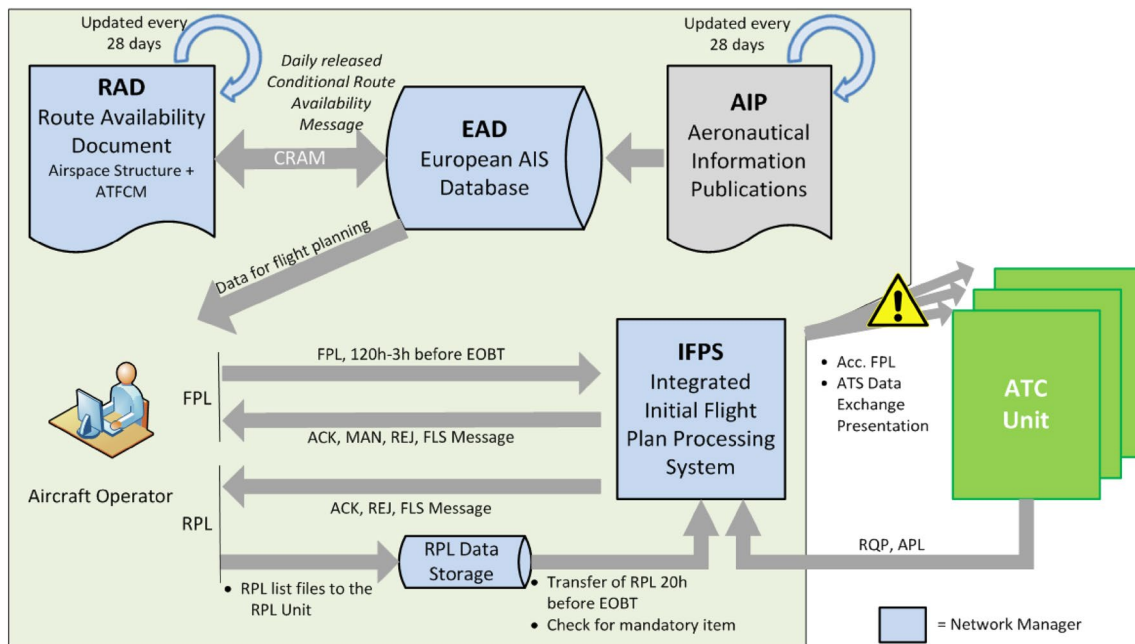
All flights simulated with TrafficSim to/from Munich follow defined Area Navigation (RNAV) departure and arrival routes, see Fig. 1. All flight-relevant information (e.g., coordinates for all fixes) is available in a navigation database. Route information for runways 26R and 26L is extracted from IFR charts, AIP 02-04-2015.

In Fig. 2, the grey rectangle represents the path stretching area used as maneuvering area for the arrival manager and by the simulated controller to compensate deviations from flight plans. The standard route uses fix DM429 to turn from the downwind leg towards the centerline. The TrafficSim uses a “Trombone” shaped path stretching area with inner



**Fig. 1** TrafficSim GUI shows the used FMS RNAV arrival routes for airport EDDM with transition BETOS 26, LANDU 26, NAPSA 26, and ROKIL 26





**Fig. 3** Flight plan data process. *ATFCM* air traffic flow and capacity management, *AIS* aeronautical information services, *EOBT* estimated off-block time, *RQP* request flight plan message, *APL* ATC flight plan message

The process of how a flight plan is prepared is pictured in Fig. 3 according to [38]. The aircraft operator prepares a flight plan based on information available from the European Aeronautical Information System Database (EAD). This information includes notably route availability data from the Route Availability Document (RAD), i.e., flow and capacity restrictions on routes, for example, city-pair-level-capping restrictions between flight information regions and airport groups, and other aeronautical information provided by the states. A flight plan can be filed for a unique flight (FPLs) or for a series of repetitive flight plans (RPL). The operator files the flight plan in Europe into the Integrated Initial Flight Plan Processing System (IFPS), a central European system. After positive validation, the IFPS will confirm the plan and copy relevant flight plan information to the affected ATC units. Normal system behavior assumes that the different copies of the flight plan data are identical.

Two different cases of attacks were implemented. In the first scenario, the defined cruise flight level is reduced in the manipulated flight plan. We consider two different variants of this scenario: (1) flight plans are manipulated for all aircraft with a certain airway and (2) flight plans are manipulated for all aircraft of a certain airline. In the second scenario, flight plans of certain departures at Munich airport are completely deleted shortly before take-off. The two scenarios with the three different targets are listed in Table 3.

**Table 3** Implemented scenarios

Type	Target
Level capping	All aircraft with certain <i>airway</i> All aircraft of certain <i>airline</i>
Deleted flight plans	Departures in Munich

Level-capping restrictions are defined in the RAD for certain airports; thus, a restriction of the flight level is not an unusual event. In addition, interviews with experts confirm that a missing flight plan is within the scope of experience of an air traffic controller. Both could be remain undiscovered as an attack for a long time.

#### 4.1 Level-capping scenario—airway

The flight plan distributed to the ATC Units is manipulated by reducing the flight level to a lower altitude. However, the operational flight plan of the cockpit crew remains unchanged. An interesting issue here is that the fuel planning is done by the crew based on their operational flight plan and thus is calculated assuming the higher flight level. If the crew is forced by ATC to remain on the lower level, a flight delay and/or unexpected additional fuel consumption occurs. The higher fuel consumption could enforce the flight crew to decide either to divert to the next suitable airfield or to continue the flight to the destination under “commitment to proceed”.

In the airway variant of the level-capping scenario, the targets are all aircraft using segments of the airway UL607 between London and Frankfurt. A restriction is already in place for some city pairs connected via UL607 according to the RAD (2007). For example, flights from London Heathrow to Frankfurt are restricted to stay in lower airspace.

Transatlantic flights would not be possible if a lower altitude is flown the whole route due to fuel consumption. For those flights, the level capping starts 500 NM before reaching the waypoint SPI at the airway UL607. This waypoint is located in Belgium, northeast of the Liège airport.

We assume that all controllers reject further climb requests by the pilot (worst-case).

In this scenario variant, an attacker tries to decrease the performance of the aviation system by causing higher flight costs (measured in increased flight time and fuel consumption), higher sector load (higher traffic density in sectors), and/or increased number of critical situations (number of conflicts).

#### 4.2 Level-capping scenario—airline

The manipulation of the flight plan is equivalent in both variants of the level-capping scenario. However, in the airline variant, the targets are aircraft of one specific airline instead of aircraft using a certain airway. The fictional airline “ARIEL-Air” operates 450 Europe domestic flights. These flights are randomly chosen out of the baseline scenario. The aircraft types in the fleet are shown in Table 4.

The potential aim of the attacker in this scenario variant is to specifically harm one airline by increasing flight costs, delaying flights and causing reputational damage.

#### 4.3 Flight plan deletion scenario

In this scenario, selected flight plans with departures in Munich are deleted in the flow management system. Multiple flight plans of an outbound rush are selected and shifted

into an inbound rush. In our experiments, an outbound rush consists of at least seven departures. In this sequence, not more than one arrival is allowed.

Such missing flight plans cause inconsistencies during start-up requests and result in “Flight plan not available” and “Contact company” messages. The flight plan needs to be filed again by the company to the IFPS; otherwise, the start-up request will not be granted.

In this scenario, the potential aim of the attacker is to shift departures into an inbound rush, so that arrivals are also delayed. The shifting could result in an overload of the airport capacity causing further delayed flights.

## 5 Simulation results

This section discusses the effects of the two attack scenarios as observed in our simulation runs. Due to the differences in the scenarios, the analyses partly contain different parameters. To support the interpretation of the simulation results, we classify the context in the following.

For the level-capping scenario, it is worth mention that fuel consumption and flight time could change significantly due to lower altitude and lead to fuel emergencies. The effects on the aircraft are evaluated for all flights affected by cyber attacks. Besides the impact on an aircraft directly, the reduced FL changes the used airspace sectors and, therefore, influences the controller workload, as well (especially if only one airway is attacked).

For the prediction of controller workload, different models exist, e.g., in RAMS (Re-organised ATC Mathematical Simulator) [39] and TAAM (Total Airspace and Airport Modeller) [38, 39]. To estimate controller workload, only tasks that can be directly derived from TrafficSim data are available. In RAMS, a controller task-time model is used (different tasks are assigned a specified number of seconds necessary to execute each task). This results in the working time of one controller. Such a model is not part of TrafficSim. Tasks considered in RAMS are:

- flight data management;
- coordination;
- conflict search;
- routine R/T (radio communication);
- radar tasks.

In TAAM, workload points represent the workload for a whole sector. Parameters for workload in TAAM are:

- movement;
- conflict;
- coordination;
- level changes.

**Table 4** Aircraft types of fictional airline “ARIEL-Air”

Boeing	B738	207
	B737	32
	B733	17
	B734	6
	B752	2
Airbus	A320	63
	A319	86
	A321	4
	A332	1
Fokker	F100	21
	F70	11



Estimated tasks for the level-capping scenario on specified airway are aircraft movements, conflict handling, and level changes.

For the level-capping scenarios, it is unknown if and at what time pilot and air traffic controller would coordinate a climb to leave the low altitude of the manipulated flight plan. Therefore, the effected flights remain at the low altitude during the whole cruise phase of flight. The scenarios are worst-case scenarios that probably do not occur in reality, due to monitoring in the cockpit and the coordination with ATC to ensure a safe flight. Nevertheless, these scenarios cause economical costs and higher resource consumption as originally planned (sector workload overload).

For the Flight Plan Deletion Scenario, the focus is on the sequence of arrivals and departures at Munich airport. In this case, we measure lost airport capacity, provoked delays and additional fuel consumption.

### 5.1 Level-capping scenario—airway

In this scenario variant, flights using the airway UL607 are targeted by cyber attacks, i.e., the flight level information is reduced to FL250 for the controllers of those flights.

The fuel calculation prior to the flight by the air carrier guarantees a safe flight in planned cruise FL to the arrival airport. The fuel consumption rises if a lower altitude than planned is enforced. In addition, fuel consumption depends on the weight carried: the less fuel, the less is the weight of the aircraft and the less fuel is needed. Therefore, to save on overall fuel consumption, fuel reserves are typically reduced to a minimum.

The affected flights are mainly taking off from United Kingdom, Belgium, Ireland, United States and Canada. The

main target destinations in Germany are Frankfurt, Munich and Düsseldorf. The resulting accumulated values for all flights via airway designated UL607 are shown in Table 5, separated by departure and arrival area. Results outlined are shown relatively to the baseline scenario. The minimum final reserve fuel (MFRF) allows a 30 min holding in 1500 ft over the alternate airport [40, p. 4.3.6.3.1]. The minimum diversion fuel (MDF) is the sum of final reserve fuel plus an alternate fuel for 150 NM (alternate aerodrome is unknown).

The amount of additional fuel caused by the lower cruise flight level is high with 1073 t in total. The related accumulated additional flight time is shown in column four. Note that additional delays and fuel consumption caused by necessary diversions are not included. However, it is shown that most of the aircraft affected by cyber attacks would exhaust their minimum diversion fuel before reaching their final destination airport. 45% (138 flights) of German overflights departing in Europe (Europe/Other) would need to divert, because even the final reserve fuel would be spent before landing. Apart from the massive economic consequences, there is also a high negative environmental impact.

The different utilization of sectors Nattenheim (NTM) FL245-325, Frankfurt (FFM) FL245-315, and Würzburg (WUR) FL245-315 are shown in Table 6. The largest increase is estimated for sector NTM. The number of conflicts significantly increases due to higher traffic volume. In addition, the traffic situation is more complex due to an increased number of multiple conflict areas and a conflict solution probably requires more controller workload. Within the ARIEL simulation, no en-route flow management tool for capacity balancing is used, thus no additional delays are caused.

**Table 5** Results of level-capping scenario for all flights on airway UL607

Departure	Arrival	No. of flights	Additional flight time	Average deviation	Additional fuel (t)	No. of flights with less than		
						MDF	MFRF	50 kg
Europe	Germany	89	02:38:07	01:46 (2.4%)	+22 (+7.8%)	53	0	0
Europe	Other	304	46:55:59	09:15 (4.2%)	+864 (+15.6%)	301	138	52
Other	Germany	65	14:25:07	13:18 (2.6%)	+98 (+2.7%)	20	0	0
Other	Other	15	09:17:44	37:10 (5.5%)	+89 (+8.3%)	15	9	8

**Table 6** Analysis of sectors Nattenheim (NTM), Frankfurt (FFM), and Würzburg (WUR)—average values are calculated from 5 a.m. till 11 p.m. for all flights on airway UL607

Sector	Aircraft per day			Average residence time (m:ss)			Average number of aircraft per minute			Number of conflicts (single and multiple)		
	NTM	FFM	WUR	NTM	FFM	WUR	NTM	FFM	WUR	NTM	FFM	WUR
Baseline	446	932	855	4:34	5:46	4:40	1.4	4.0	3.0	24	87	63
Level capping	780	1197	1081	6:06	5:48	5:32	3.9	5.3	4.6	65	118	117
										7	18	21

## 5.2 Level-capping scenario—airline

This scenario variant focuses on the economic impact of the level-capping cyber attack on a single airline.

The simulation results according to fuel consumption and flight time are shown in Table 7. All results outlined are relative to the baseline scenario. Comparing Table 7 and column three of Table 6, the additional flight time is increased by 26 min. This is caused by the mix of attacked aircraft types with a high percentage of Boeing jets (Table 4). The airspeed of a Boeing below Mach transition altitude is comparatively low, e.g., the nominal airspeed of a Boeing 738 in FL250 is only 280 kts. Nevertheless, 5 min delay in average seems to be negligible. However, it needs to be considered that additional delays and fuel consumption caused by necessary diversions are not included in the listed values. According to the fuel consumption, most of the attacked flights would exhaust diversion fuel before reaching their final destination airport. At least 15 aircraft have to divert, because their landing fuel would be below the final reserve fuel.

With a daily traffic volume of about 30,000 flights (25,000–33,000) over Europe some additional questions would have to be discussed like: how long would it take to detect a cyber attack affecting only 450 flights? Moreover, how long would the airline need to detect that the problems occur due to a cyber attack? Suppose this attack happens only once per month or only to a few aircraft, the attack could remain undetected for a long time. However, the accumulated additional fuel consumption will result in a massive economic damage for the airline “ARIEL-Air”.

## 5.3 Flight plan deletion scenario

This scenario focusses on departures and arrivals at Munich airport only, more precisely at runway 26R. Flight plans are deleted by an attack and must be refiled and rescheduled. The goal is to measure the delays and to show how long that will affect the scenario day.

The attack is performed in two different variants:

- The first variant has four missing flight plans and the delay of rescheduling has a fixed duration. That is performed once.
- The second variant has five missing flight plans and the delay values were randomly determined by a triangular

distribution. That was simulated in 100 runs with the same outbound rush.

For each variant, the number of delayed flights, the accumulated delay time, maximum delay, and additional fuel consumption, respectively the average mean (AM), were calculated.

Based on expert assessment, we assume the expected delay for the startup, caused by the re-filing of the missing flight plan, is 10–20 min. Considered in these minutes are the communication between pilot and air traffic controller, company contact from pilot, creation of new flight plan with acknowledgements from the IFPS, and the upload of the new flight plan to the aircraft. All rescheduling and adaptations caused by new take-off or touchdown times are managed by TrafficSim to meet time constraints and keep all trajectories safely separated.

In the following paragraphs the first variant is described in detail, while the second variant merely presents the results afterwards.

### 5.3.1 Variant with four missing flight plans

We assumed that the attacks occur, while the occupancy rate of runway 26R is high. For example, out of seven departures (outbound rush), DEP1 to DEP7, every second flight plan is deleted. The selected outbound rush starts at 6:38 a.m. and ends at 6:48 a.m. The first flight, DEP1, gets a rejection at start-up time  $t_0$  justified with the message “no ATC flight plan available”. Assuming that a new flight plan is filed after 15 min, the AMAN/DMAN sequence planning reinserts the delayed DEP1 in the arrival and departure traffic stream at 6:53 a.m. Flights after that time need to be postponed, because there is no buffer available until noon. To meet updated time constraints by the tactical tools AMAN and DMAN arrival routes are shortened or extended using the path stretching area (grey area in Fig. 2). The sequence of surrounding flights is always maintained. Thus, the AMAN/DMAN sequence planner checks arrivals between  $t_0$  and  $t_0 + 15$  min whether an early landing is possible or not. Directly following departures are not yet ready for startup and are not advanced. In case of DEP1, following arrivals are not able to shorten their route that much, resulting in a gap in the departures outbound rush between 6:39 a.m. and 6:42 a.m. This resulting gap represents loss of capacity for the airport.

**Table 7** Simulation results of the level-capping scenario—airline

No. of flights	Additional flight time	Average deviation	Additional fuel (t)	% Total fuel	No. of flights with less than		
					MDF	MFRF	50 kg
450	14:51:04	05:10 (5.5%)	215	11.4	327	15	0

**Table 8** Re-planning result initiated via “flight plan deleted” incident of four flight plans in an outbound rush of seven departures

	Late	Delay	Flight delay	Max. delay	Additional fuel
Arrival	77	01:20:01	00:01:02	00:04:01	2.3 t
Departure	95	03:00:23	00:01:53	00:19:04	–

**Table 9** Average mean of 100 samples of re-planning results initiated via “flight plan deleted” incident of five flight plans in an outbound rush of nine departures

	AM late	AM delay	AM flight delay	Max. delay	AM additional fuel
Arrival	39	00:59:51	00:01:33	00:08:45	1.2 t
Departure	35	03:03:49	00:05:20	00:26:33	–

To reschedule DEP1 at  $t_0 + 15$  min, following departures or arrivals are postponed so that DEP1 can take place. Those shifted flights are now delayed.

The whole process is iterated for DEP3, DEP5, and DEP7. The time until these flights were rescheduled is set to 16, 17, and 18 min delay. The results of the whole attack are summarized in Table 8. The accumulated delay includes late and early flights. The total delay is, therefore, 04:20:24 h. Any rescheduled missing flight plan will iteratively increase the delay of subsequent flights as long as no buffer can be used. The resulting maximum delay of an arrival is 4:01 min and for a departure it is 19:04 min. Additional fuel for departures is not calculated, because its arrival airports are not under observation.

The scenario day is affected by the attack for a duration of 4:15:58 h (impact period) until the simulation is back to normal operational state according to the Baseline Scenario.

### 5.3.2 Variant with five missing flight plans

The second variant of five deleted flight plans out of one specified departure block with nine successive departures was simulated a hundred times with the same outbound rush. This outbound rush starts at 11:28 am. The average mean (AM) delay and additional fuel out of these 100 samples are shown in Table 9. The total average delay accumulates to 4:03:40 h.

The impact period here is in mean 1:54:18.

### 5.3.3 Discussion of the variants

In the first variant, almost twice as much fuel is consumed with a delay of only 20 min more. This is due to shorter level phases before the last descent when approaching the airport.

It is noticeable that the impact period with five deleted flight plans is shorter than for four deleted flight plans. The first attack variant begins at 06:38 a.m., while the second begins at 11:28 a.m. On runway 26R, almost no free capacity is available between 6:00 a.m. and noon. Thus, in the first variant, more flights have to be rescheduled to reinsert the attacked flights into the arrival and departure sequence (see number of late flights in Tables 8 and 9).

## 6 Discussion

In this section we discuss the results of our simulations and state arising further research questions. Based on our simulation results, we derive recommendations to strengthen the cyber resilience of the air traffic system.

We investigated the benefit of simulation to support cyber attack impact analysis as a basis for the improvement of cyber-resilience, we simulated scenarios, where the integrity and the availability of flight plan data are violated. In the scenario, where integrity is compromised, we assume that an attacker deliberately manipulates the flight level. In the airway variant of the level-capping scenario, the attacker manipulates flight levels for aircrafts passing the airway UL607 to disturb the general air traffic. In the “ARIEL-Air” variant, the cyber attacker targets a fictional airline “ARIEL-Air” by manipulating the flight level for aircraft from this airline only.

For both scenarios, we had to specify the details of the flight level manipulation. Although the impacts of varying types of manipulations would differ, we demonstrate that marginal manipulations can have significant influence on the overall flight operations. We observed significant increases of delays and fuel consumption, even with the potential of provoking air safety incidents (i.e., fuel emergencies). In addition, we observed shifts and increases of ATC workload up to exceeding sector capacity. The Flight Plan Deletion Scenario focuses on a violation of the availability of flight plan data. We assume that an attacker deletes certain flight plans with departures from Munich, in the Flow Management System. We show that even the deletion of a few flight plans could have a significant impact on the overall operation. The deletion of four (five, resp.) flight plans, out of a departure block with nine successive departures, leads to a dramatic increase of average delay for arrivals and departures. In this specific example, it takes 4 (2, respectively) h for the system to be back in normal operation.

Due to project time and resource restrictions, we had to work with simplifications and assumptions. For example, our employed simulation model only considers airborne processes. There is no simulated interaction with planning or ground processes. Thus, effects propagating beyond aircraft turnarounds are not observable with the help of our model. In addition, we are not able to study the impacts on the downstream logistics chain caused by delays or higher fuel consumption and their possible impacts back to airborne processes. The simulation model also neglects any human interactions during the simulation.

However, especially for the “ARIEL-Air” variant of the level-capping scenario, where we manipulated only 450 flight plans out of about 30,000 flights over Europe, further research questions are raised, e.g.:

- How would the discussion with the controller look like?
- Would a pilot really stay that long in a lower flight level?
- How long would it take to detect the cyber attack?
- How long would the airline need to detect that the problems occur due to a cyber attack?

The results of our simulations imply also a strong impact on the downstream logistics chain. Due to delayed aircrafts, passengers can miss connection flights. These passengers possibly need alternative transportation or even accommodation. Thus, the simulated manipulations caused by cyber attacks are propagating far beyond our defined simulation model boundaries. They cause significant impacts in all connected systems. In consequence, besides developing simulation models to evaluate, study and quantify systems under cyber attack, we recommend to integrate human interactions and connect simulation models from gate to gate.

We summarize and discuss our experiences collected during our research in the form of recommendations in the following Section.

## 6.1 Recommendations

The working results developed in the context of the ARIEL-Sim project (our executed simulations and the corresponding simulation results) give rise to the following recommendations to strengthen the cyber-resilience of the air traffic system. Although not explicitly addressed in the project, we are confident that our recommendations are also valid for other domains, especially in the area of critical infrastructures. The following recommendations found their way into the recommendations document of project ARIEL [41].

### 6.1.1 Develop, maintain, and apply simulation models and cyber attack simulation scenarios

To achieve a holistic understanding of the effects of potential cyber attacks in complex systems, simulation is a valuable alternative to more traditional analysis methods. We recommend a more wide-spread application of simulation models for processes and systems identified by cyber-threat and risk analysis as critical for the system operation. Simulation increases the understanding of the impact of identified cyber threats and supports the validation of risk analysis results. The increase in understanding of impacts and effects is the basis for the development of effective countermeasures, for example, algorithms and methods for early warnings about potential cyber attacks.

In addition, we recommend to maintain and to use existing simulation models for cyber-threat and risk analyses. Our research shows that simulation models of airborne processes do not necessarily need a special design to support a wide range of experiments regarding cyber attacks. We assume that this observation is valid in other domains outside the aviation sector, as well. A simulation experiment is based on scenarios, where the concrete data manipulation has to be identified and specified. Therefore, it is important to develop valid simulation scenarios. Interdisciplinary teams that are able to provide a comprehensive consideration of attacker motivation and attack impacts should develop these scenarios.

Furthermore, we recommend to use simulation results for cyber-security awareness building, especially for task-specific security awareness trainings. Beyond basic awareness, simulation can also be exploited to support decision-making and planning processes, by exposing the respective staff to the data produced by simulation.

### 6.1.2 Connect and develop simulation models from “gate-to-gate”

Most existing simulation models focus on a special area of application. Potential propagations of effects beyond the boundaries of operational processes are usually difficult to observe and analyse. For example, the evaluation of the impacts on ground processes or strategic planning processes resulting from a cyber attack to the overall chain of processes needs integrated and connected simulation models. We recommend to identify, to specify and to develop the needed connections between simulation model boundaries.

### 6.1.3 Integrate human interactions with cyber attack simulation scenarios

A comprehensive cyber attack simulation program needs HITL simulations. These require human interactions during

the simulation execution, notably to evaluate the impact of communication and coordination of controllers and pilots. In the case of closed-loop simulation, typical user interactions need to be modelled with assumptions or simplifications. Especially in the area of air traffic management and flight execution, the assumptions on these interactions influence the results of a simulation significantly.

We recommend to integrate human interactions within cyber attack simulations to increase the validity, quality, and significance of the results of the simulations and to study and observe the behavior of humans interacting with a system under cyber attack. For example, the execution of cockpit and ATC workstation simulation allows the measurement of negotiation, reaction and action times. It requires the staffing of the simulations with personal with operational skills. This will improve existing and support the development of new simulation models. Moreover, the results of human-in-the-loop simulations will support the elaboration and development of user requirements for systems susceptible to potential cyber attacks. This will enlighten the currently ongoing discussion about the essential future skills of operational staff to identify and manage cyber attacks. Since HITL simulations are also prevalent in the area of education and training, we recommend to integrate cyber attack simulation scenarios within these training programs to support and improve the development and implementation of codes of conduct to face potential cyber attacks.

## 7 Conclusion

In our work we investigated the potential of simulation to support the understanding of the consequences in potential cyber-threat situations in connection with flight plan data processing. Despite simplifications and assumptions, also considering data sources from other years, we show that simulation is a valid methodology to investigate impacts of cyber attacks to the air traffic system. Our simulations showcase general impacts and how they propagate through the system in time. We demonstrated that small manipulations could even cause safety critical incidents. In the level-capping scenario 45% (138 flights) would need to divert caused by consumption of the final reserve fuel and out of these 52 flights would not reach their final destination. Simulation allows us to evaluate the criticality of manipulations and support a deeper understanding of the air traffic system under cyber attack. However, our collected experiences, which we summarized in recommendations, show that there are applications of simulation which we could not address in our research due to time and resource restrictions. Especially the integration of human interactions with the simulation scenarios allows the evaluation of further research questions.

Our simulations were not planned as human-in-the-loop simulations and do not involve any countermeasures, e.g., an air traffic controller could make. Our results show the effects of the scenarios without human actions.

The flight plan deletion scenario showed that the results (e.g., impact period) are mainly dependent on the scenario in use and the time of the attack. To determine a generally valid value, further simulation runs with different scenario days would have to be performed.

An additional focus in the field of simulation-supported risk analysis should be the development of needed interfaces between simulation model boundaries to study effects beyond the boundaries of operational processes.

**Acknowledgements** This paper presents some of the results of the ARIEL (Air Traffic Resilience) project supported by the Bavarian State Ministry of Economics, Media, Energy, and Technology (Grant no. LABAY84C) as part of the Bavarian Aviation Research Program. We would like to thank the partners of the ARIEL project for their general support in the work that led to this paper. Thanks to the DFS for their support and for collecting expert opinions.

## References

1. Kölle, R., Markarian, G., Tarter, A.: *Aviation Security Engineering: A Holistic Approach*. Artech House, Norwood (2011)
2. Zetter, K.: All U.S. united flights grounded over mysterious problem. WIREd. <https://www.wired.com/2015/06/united-flights-grounded-mysterious-problem/> (2015)
3. SecurityWeek: Hackers target polish airline LOT, ground 1,400 passengers. <http://bit.ly/1daLI9X> (2015). Accessed 2017
4. Peltier, T.: *Information Security Risk Analysis*, CRC Press, Boca Raton (2005)
5. Heinemann, P., Jeßberger, C., Knoll, A., Cole, M.: *Air Traffic Resilience Scenarios*. presented at Deutscher Luft- und Raumfahrtkongress, Rostock (2015) (**unpublished**)
6. Kiesling, T., Krempel, M., Niederl, J., Ziegler, J.: A model-based approach for aviation cyber security risk assessment. In: Presented at 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria (2016) (**unpublished**)
7. Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., Martinovic, I.: On perception and reality in wireless air traffic communication security. *IEEE Trans. Intell. Transp. Syst.* **18**:1338–1357 (2017)
8. McAllister, N., No, You, C.A.N.T., Hijack, A.: *Plane with an android app*. <http://goo.gl/nUoFP3> (2013). Accessed 2018
9. Polstra, P., Polly, C.: *Cyber-hijacking airplanes: truth or fiction*. In: Presented at Proceedings of 22nd DEFCON (2014) (**unpublished**)
10. Walker, G.: *Is air traffic control a soft target for hackers?* <http://goo.gl/zDy3rE> (2013). Accessed 2018
11. Warkentin, M., Willison, R.: Behavioral and policy issues in information systems security: the insider threat. *Eur. J. Inf. Syst.* **18**, 101–105 (2009)
12. Loffi, J., Wallace, R.: The unmitigated insider threat to aviation (part 1): a qualitative analysis of risks. *J. Transp. Secur.* **7**, 289–305 (2014)
13. Rabe, M., Spieckermann, S., Wenzel, S.: *Verifikation und Validierung für die Simulation in Produktion und Logistik: Vorgehensmodelle und Techniken*. Springer Science & Business Media, Berlin (2008)

14. Wenzel, S., Weiß, M., Collisi-Böhmer, S., Pitsch, H., Rose, O.: Qualitätskriterien für die Simulation in Produktion und Logistik: Planung und Durchführung von Simulationsstudien. Springer, Berlin 2007
15. Haßa, O.: Eine anwendungsorientierte Einführung in ATM-Simulationen, Langen: Innovation im Fokus. DFS Deutsche Flugsicherung, Langen (2016)
16. Schwentek, K.: Kopplung zwischen einem Schnellzeitsimulationstool und betrieblichen Planungssystemen der DFS. TE im Fokus 2006, pp. 26–40 (2006)
17. Silverio, I., Juan, A., Arias, P.: A simulation-based approach for solving the aircraft turnaround problem. In: Fernández-Izquierdo, M.Á., Muñoz-Torres, M.J., León, R. (eds.) Modeling and simulation in engineering, economics, and management. MS 2013. Lecture Notes in Business Information Processing, vol. 145, pp. 163–170. Springer, Berlin, Heidelberg (2013)
18. Prevot, T., Lee, P., Callantine, T., Mercer, J., Homola, J., Smith, N., Palmer, E., Human-in-the-loop evaluation of NextGen concepts in the Airspace Operations Laboratory. In: Proceedings of the AIAA Modeling and Simulation Technologies (MST) Conference, Toronto, Canada (2010)
19. EUROCONTROL: Real time simulations. <http://www.eurocontrol.int/articles/real-time-simulations>. Accessed: 2017
20. Law, A.M., Kelton, W.D.: Simulation & Modeling Analysis. MacGraw-Hill Education, New York (2014)
21. Johansson, M., Rantzer, A.: Computation of piecewise quadratic Lyapunov functions for hybrid systems. IEEE Trans. Autom. Control **43**, 555–559 (1998)
22. Zeigler, B., Praehofer, H., Kim, T.: Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems. Academic Press, Boca Raton (2000)
23. Brailsford, S., Desai, S., Viana, J.: Towards the holy grail: combining system dynamics and discrete-event simulation in healthcare. In: Simulation Conference (WSC), Proceedings of the 2010 Winter, Simulation Conference (WSC), Proceedings of the 2010 Winter, IEEE (2010)
24. Ekyalimpa, R., Werner, M., Hague, S., AbouRizk, S., Porter, N.: A combined discrete-continuous simulation model for analyzing train-pedestrian interactions. In: IEEE, Winter Simulation Conference (WSC), 2016 (2016)
25. Forrester, J.: Counterintuitive behavior of social systems. Technol. Forecast. Soc. Change **3**, 1–22 (1971)
26. Wooldridge, M.: Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence. MIT Press, Cambridge (1999)
27. Cohen, F.: Simulating cyber attacks, defenses, and consequences. Comput. Secur. **18**, 479–518 (1999)
28. Chi, S.D., Park, J., Jung, K.C., Lee, J.S.: Network security modeling and cyber attack simulation methodology. In: Varadharajan, V., Mu, Y. (eds.) Information security and privacy. ACISP 2001. Lecture Notes in Computer Science, vol. 2119. Springer, Berlin, Heidelberg (2001)
29. Ekelhart, A., Kiesling, E., Grill, B., Strauss, C., Stummer, C.: Integrating attacker behavior in IT security analysis: a discrete-event simulation approach. Inf. Technol. Manag. **16**, 221–233 (2015)
30. Stelkens-Kobsch, T., Finke, M., Kleinert, M., Schaper, M.: Validating an ATM security prototype—first results. In: 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento (2016)
31. Monteiro, M., Sarmento, T., Barreto, A., Costa, P., Hieb, M., An integrated mission and cyber simulation for air traffic control. In: Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on, pp. 2687–2692 (2016)
32. EUROCONTROL: User Manual for the Base of Aircraft Data (BADA) Revision 3.12. European Organization for the Safety of Air Navigation EUROCONTROL, Brussels (2014)
33. Geister, D., Schwoch, G., Geister, R., Korn, B.: Integrating RPAS into Existing ATM Structures—Published Approach Procedures vs. Local Arrangements. ICNS, Herndon (2017)
34. Czerlitzki, B.: The experimental flight management system: advanced functionality to comply with ATC constraints. Air Traffic Control Q **2**, 159–188 (1994)
35. Boguhn, O., Basner, M., Enghardt, L., Dobrzynski, W., König, R., Kuenz, A., Stump, R., Isermann, U., Heimann, D.: DLR-Projekt ‘Leiser Flugverkehr II. Abschlussbericht, Göttingen (2017)
36. Kuenz, A., Peinecke, N.: Effiziente 4D-Konflikt-Erkennung für großräumige Szenarien, Verfahren zur Ermittlung einer potenziellen Konfliktsituation, EP 2 457 224 A2 (2011)
37. Kuenz, A., Peinecke, N.: Method for determining a potential conflict situation. US 20120158278, Jun 2012
38. Cook, A.: European Air Traffic Management—Principles, Practice and Research. Ashgate, Farnham (2007)
39. Sillard, L., Vergne, F., Desart, B.: TAAM operational evaluation. Eurocontrol Experimental Centre, EEC Report 351 (2000). [https://www.eurocontrol.int/eec/public/standard\\_page/DOC\\_Report\\_2000\\_022.html](https://www.eurocontrol.int/eec/public/standard_page/DOC_Report_2000_022.html)
40. International Civil Aviation Organization: Annex 6 Part I—Operation of Aircraft, 8th ed. ICAO (2001)
41. Kiesling, T., Ziegler, J., Rieth, T., Schupke, D., Exposito-Garcia, A., Biermann-Höller, S., Krempel, M., Schuster, D., Dreo Rodosek, G., Bierwirth, T., et al.: Recommendations to Strengthen the Cyber-Resilience of the Air Traffic System, 2nd ed. Ottobrunn (2017). [http://lbcampus.de/images/content/ARIEL\\_Recommendations\\_v2.0.pdf](http://lbcampus.de/images/content/ARIEL_Recommendations_v2.0.pdf)